9110-9P

DEPARTMENT OF HOMELAND SECURITY

National Protection and Programs Directorate; Cybersecurity Information Sharing Act of 2015 Interim Guidance Documents – Notice of Availability

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: Notice of availability.

SUMMARY: DHS is announcing the availability of Cybersecurity Information Sharing Act of 2015 Interim Guidance Documents jointly issued with the Department of Justice (DOJ) in compliance with the Act (CISA), which authorizes the voluntary sharing and receiving of cyber threat indicators and defensive measures for cybersecurity purposes, consistent with certain protections, including privacy and civil liberty protections.

ADDRESSES: The CISA guidance documents may be found on www.us-cert.gov/ais.

FOR FURTHER INFORMATION CONTACT: If you have questions about this notice, email Matthew Shabat at matthew.shabat@hq.dhs.gov or telephone on (703) 235-5338. Questions may also be directed by mail to Matthew Shabat, 245 Murray Lane, S.W., Mail Stop 0610, Washington, DC 20528-0610.

SUPPLEMENTARY INFORMATION: The CISA requires the Secretary of DHS and the Attorney General to jointly develop and make publicly available –

- guidance to assist non-Federal entities and promote sharing of cyber threat indicators with the Federal Government;
- interim and final guidelines for the protection of privacy and civil liberties; and
- interim and final procedures related to the receipt of cyber threat indicators and defensive measures by the Government, which happen principally through the

real-time DHS process, the existing DHS-operated Automated Indicator Sharing (AIS) initiative and may also occur through direct submissions to Federal agencies.

The CISA also requires the Secretary of DHS, the Attorney General, the Director of National Intelligence, and the Secretary of Defense, to jointly develop interim procedures to facilitate and promote the sharing of cyber threat indicators and defensive measures by the Federal Government.

Authority and Background

On December 18, 2015, the President signed into law the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, which included at Division N, Title I the Cybersecurity Information Sharing Act of 2015 (CISA). Congress designed CISA to establish a voluntary cybersecurity information sharing process that encourages public and private sector entities to share cyber threat indicators and defensive measures while protecting privacy and civil liberties. The CISA requires various Executive Branch agencies to coordinate and create, within 60 days of enactment (i.e., not later than February 16, 2016), four guidance documents to facilitate this voluntary cybersecurity information sharing process. The CISA requires two of these interim documents to be made publicly available. See generally Pub. L. No. 114-113, Div. N, Title I secs. 103, 105).

Overview of the 60 Day Guidance Required under CISA

The CISA sec. 103 requires the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation

with the heads of designated Federal entities,[1] to jointly develop and issue procedures to facilitate and promote the sharing by the Federal Government of classified and unclassified cyber threat indicators, defensive measures, and other information and best practices related to mitigating cyber threats. The CISA sec. 103(b) requires these procedures to include a real-time sharing capability (namely the DHS Automated Indicator Sharing (AIS) initiative); incorporate existing Federal information sharing processes, procedures, roles, and responsibilities to the greatest extent possible; account for sharing done in error; and protect against unauthorized access to cyber threat information. Further, the procedures must account for the review of cyber threat indicators to identify personal information not related to the threat, a technical capability to remove such personal information, and a notification process to alert any U.S. person whose personal information is improperly shared by a Federal entity.

The CISA sec. 105(a)(1) requires the Secretary of Homeland Security and the Attorney General, in consultation with the heads of designated Federal entities, to jointly develop and issue interim policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government. These internal operational procedures describe general rules applicable to DHS and other Federal agencies and the operative processes of the DHS AIS system, including the statutory requirement for Federal agencies that receive cyber threat indicators and defensive measures to share them with other appropriate agencies.

The CISA sec. 105(a)(4) requires the Secretary of Homeland Security and the

[1] The CISA defines Appropriate Federal Entities as the Departments of Commerce, Defense, Energy, Homeland Security, Justice, Treasury, and the Office of the Director of National Intelligence. See CISA sec. 102(3).

Attorney General to jointly develop and make publicly available guidance to assist non-Federal entities with sharing cyber threat indicators with Federal entities. This guidance includes explanations of how non-Federal entities can identify and share cyber threat indicators and defensive measures with the Federal Government in accordance with CISA and describes the protections non-Federal entities receive under CISA for sharing cyber threat indicators and defensive measures, including targeted liability protection and other statutory protections.

Finally, CISA sec. 105(b) requires the Secretary of Homeland Security and the Attorney General, in consultation with the Department Heads and Chief Privacy and Civil Liberties Officers of the designated Federal entities, to jointly develop and make publicly available interim guidelines relating to privacy and civil liberties that govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity. These privacy and civil liberties guidelines are consistent with the Fair Information Practice Principles (FIPPs) set forth in Appendix A of the "National Strategy for Trusted Identities in Cyberspace," published by the President in April 2011.

Issuance of Agency Guidance required under CISA

The CISA guidance documents may be found on www.us-cert.gov/ais.

Dated: February 11, 2016. .

Andy Ozment,
Assistant Secretary,
Department of Homeland Security.
[FR Doc. 2016-03430 Filed: 2/17/2016 8:45 am; Publication Date: 2/18/2016]